

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

*IN RE USAA DATA SECURITY
LITIGATION*

Case No. 7:21-cv-05813-VB

**UNITED SERVICES AUTOMOBILE ASSOCIATION'S MEMORANDUM OF LAW IN
SUPPORT OF ITS MOTION TO DISMISS**

HUNTON ANDREWS KURTH LLP
200 Park Avenue
New York, NY 10166
(212) 309-1000

*Attorneys for Defendant
United Services Automobile Association*

TABLE OF CONTENTS

I.	PRELIMINARY STATEMENT	1
II.	STATEMENT OF FACTUAL ALLEGATIONS	2
III.	ARGUMENT	4
	A. Standards of Review under Rules 12(b)(1) and 12(b)(6).....	4
	B. Plaintiffs Lack Article III Standing.....	5
	C. USAA Did Not “Knowingly” Engage in Any DPPA Violative Conduct (Count III)	7
	D. Plaintiffs Do Not State a Negligence Claim (Count I)	11
	1. New York does not recognize claims for “negligent enablement of impostor fraud”	12
	2. USAA owes no duty of care to Plaintiffs with whom it has no relationship.....	13
	E. Plaintiffs Fail to State a Negligence Per Se Claim (Count II)	16
	F. The Economic Loss Doctrine Bars Plaintiffs’ Negligence-Based Claims (Counts II and III)	17
	G. Plaintiffs Fail to State a GBL § 349 Claim (Count IV)	19
	1. Plaintiffs fail to plead sufficient causation.....	19
	2. Other asserted statutory violations do not establish a GBL § 349 claim...20	
	H. Plaintiffs Fail to Allege Cognizable Damages (Counts II, III, and IV)	21
	I. Plaintiffs Lack Sufficient Grounds for Declaratory or Injunctive Relief	23
IV.	CONCLUSION.....	25

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc.,</i> 96 N.Y.2d 280, 750 N.E.2d 1097 (2001).....	17, 18
<i>Abdale v. N. Shore Long Island Jewish Health Sys., Inc.,</i> 49 Misc. 3d 1027, 19 N.Y.S.3d 850 (2015).....	17
<i>Abdulaziz v. McKinsey & Co., Inc.,</i> No. 21 CIV. 1219 (LGS), 2021 WL 4340405 (S.D.N.Y. Sept. 22, 2021).....	13, 14
<i>Allen v. Vertfore, Inc.,</i> No. 4:20-cv-04139, 2021 WL 3144469 (S.D. Tex. July 23, 2021)	8
<i>Allen v. Vertfore, Inc.,</i> No. 4:20-cv-04139, 2021 WL 3148870 (S.D. Tex. June 14, 2021).....	6, 8, 9, 11
<i>Ambac Assurance Corp. v. U.S. Bank Nat'l Ass'n,</i> 328 F. Supp. 3d 141 (S.D.N.Y. 2018).....	17, 18
<i>Ashcroft v. Iqbal,</i> 556 U.S. 662 (2009).....	4
<i>Beck v. McDonald,</i> 848 F.3d 262 (4th Cir. 2017)	24
<i>Bell Atl. Corp. v. Twombly,</i> 550 U.S. 544 (2007).....	4
<i>Bellwether Cnty. Credit Union v. Chipotle Mexican Grill, Inc.,</i> 353 F. Supp. 3d 1070 (D. Colo. 2018).....	18
<i>Bernstein v. City of N. Y.,</i> 621 F. App'x 56 (2d Cir. 2015)	23
<i>Bibicheff v. PayPal, Inc. (Bibicheff I),</i> No. 217CV4679DRHAYS, 2020 WL 2113373 (E.D.N.Y. May 4, 2020)	12, 14, 15
<i>Bibicheff v. PayPal, Inc. (Bibicheff II),</i> 844 F. App'x 394, 396 (2d Cir. 2021)	12, 14, 19, 20
<i>In re Brinker Data Incident Litig.,</i> No. 3:18-CV-686-J-32MCR, 2020 WL 4287270 (M.D. Fla. July 27, 2020)	24

<i>Carter v. HealthPort Techs., LLC,</i> 822 F.3d 47 (2d Cir. 2016).....	4
<i>Chiste v. Hotels.com L.P.,</i> 756 F. Supp. 2d 382 (S.D.N.Y. 2010).....	23, 24
<i>Clapper v. Amnesty Int'l USA,</i> 568 U.S. 398 (2013).....	6
<i>Cmtys. Bank of Trenton v. Schnuck Markets, Inc.,</i> 887 F.3d 803 (7th Cir. 2018)	18
<i>Cohen v. Ne. Radiology, P.C.,</i> No. 20 CV 1202 (VB), 2021 WL 293123 (S.D.N.Y. Jan. 28, 2021).....	16
<i>Colangelo v. Champion Petfoods USA, Inc.,</i> No. 618CV1228LEKML, 2020 WL 777462 (N.D.N.Y. Feb. 18, 2020).....	17
<i>Conboy v. AT & T Corp.,</i> 241 F.3d 242 (2d Cir. 2001).....	20
<i>Cooper v. Bonobos, Inc.,</i> No. 21-CV-854 (JMF), 2022 WL 170622 (S.D.N.Y. Jan. 19, 2022)	5, 6
<i>Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc.,</i> 455 Mass. 458, 918 N.E.2d 36 (2009)	18
<i>Davis v. S. Nassau Cmtys. Hosp.,</i> 26 N.Y.3d 563, 46 N.E.3d 614 (2015).....	14
<i>Doe v. Minn. Dep't of Pub. Safety Does (1-10),</i> No. 17-4164(DSD/DTS), 2018 WL 1277005 (D. Minn. Mar. 12, 2018).....	8
<i>Doe v. Uber Techs., Inc.,</i> No. 20-CV-8446 (LJL), 2021 WL 3193166 (S.D.N.Y. July 28, 2021).....	19
<i>Eiseman v. State,</i> 70 N.Y.2d, 511 N.E.2d 1128 (1987).....	14
<i>Enslin v. Coca-Cola Co.,</i> 136 F. Supp. 3d 654 (E.D. Pa. 2015)	7, 8, 9
<i>Fero v. Excellus Health Plan, Inc.,</i> 236 F. Supp. 3d 735 (W.D.N.Y. 2017)	21
<i>Ferreira v. City of Binghamton,</i> 975 F.3d 255 (2d Cir. 2020).....	11

<i>Gale v. Int'l Bus. Machines Corp.</i> , 9 A.D.3d 446, 781 N.Y.S.2d 45 (2004)	20
<i>In re GE/CBPS Data Breach Litig.</i> , No. 20 CIV. 2903 (KPF), 2021 WL 3406374 (S.D.N.Y. Aug. 4, 2021)	16
<i>Greenstein v. Noblr Reciprocal Exchange</i> , No. 21-cv-04537-JSW, 2022 WL 472183 (N.D. Cal. Feb. 15, 2022)	5, 6
<i>Gulsvig v. Mille Lacs Cty.</i> , No. CIV. 13-1309 JRT/LIB, 2014 WL 1285785, at *6 (D. Minn. Mar. 31, 2014)	10
<i>Hammond v. Bank of N.Y. Mellon Corp.</i> , No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307 (S.D.N.Y. June 25, 2010)	15, 16
<i>Hensley v. City of Charlotte</i> , No. 320CV00482KDBDSC, 2021 WL 4929491 (W.D.N.C. Oct. 21, 2021)	6
<i>Holmes v. Countrywide Fin. Corp.</i> , No. 5:08-CV-00205-R, 2012 WL 2872892 (W.D. Ky. July 12, 2012)	8
<i>Irwin v. Jimmy John's Franchise, LLC</i> , 175 F. Supp. 3d 1064 (C.D. Ill. 2016)	24
<i>Kanciper v. Lato</i> , No. 13CV00871ADSWDW, 2014 WL 12847274 (E.D.N.Y. Mar. 31, 2014)	23
<i>Kiminski v. Hunt</i> , Nos. 12-185, 13-208, 13-286, 13-358, 13-389, 2013 WL 6872425 (D. Minn. Sept. 20, 2013)	8, 9, 10
<i>L-7 Designs, Inc., v. Old Navy, LLC</i> , 647 F.3d 419 (2d Cir. 2011)	4
<i>Ladino v. Bank of Am.</i> , 52 A.D.3d 571, 861 N.Y.S.2d 683 (2008)	12
<i>Loeffler v. City of Anoka</i> , No. 13-CV-2060 MJD/TNL, 2014 WL 4449674, at *6 (D. Minn. June 24, 2014)	10
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992)	5
<i>Luparello v. Inc. Vill. of Garden City</i> , 290 F. Supp. 2d 341 (E.D.N.Y. 2003)	7
<i>McCulloch v. Town of Milan</i> , 559 F. App'x 96 (2d Cir. 2014)	25

<i>McFarlane v. Altice USA, Inc.,</i> 524 F. Supp. 3d 264 (S.D.N.Y. 2021).....	17
<i>McMorris v. Carlos Lopez & Assocs., LLC,</i> 995 F.3d 295 (2d Cir. 2021).....	5
<i>In re Merrill Lynch & Co.,</i> 273 F. Supp. 2d 351 (S.D.N.Y. 2003).....	2
<i>In re Michaels Stores Pin Pad Litig.,</i> 830 F. Supp. 2d 518 (N.D. Ill. 2011)	18
<i>In re N.Y. City Asbestos Litig.,</i> 27 N.Y.3d 765, 59 N.E.3d 458 (2016).....	13
<i>Nahabedian v. Intercloud Sys., Inc.,</i> No. 15-CV-00669(RA), 2016 WL 155084 (S.D.N.Y. Jan. 12, 2016)	24, 25
<i>Nelson v. Jesson,</i> No. 13-340, 2013 WL 5888235 (D. Minn. Nov. 1, 2013)	8
<i>Norton v. Town of Islip,</i> 678 F. App'x 17 (2d Cir. 2017)	23
<i>Oddo v. Queens Vill. Comm. for Mental Health for Jam. Cnty. Adolescent Program, Inc.,</i> 28 N.Y.3d 731, 71 N.E.3d 946 (2017).....	14
<i>Perdue v. Hy-Vee, Inc.,</i> 455 F. Supp. 3d 749 (C.D. Ill. 2020)	18
<i>Polzer v. TRW, Inc.,</i> 256 A.D.2d 248, 682 N.Y.S.2d 194 (1998).....	12, 15
<i>Prignoli v. Bruczynski,</i> No. 20-CV-907 (MKB), 2021 WL 4443895 (E.D.N.Y. Sept. 28, 2021).....	20
<i>Pulka v. Edelman,</i> 40 N.Y.2d 781, 358 N.E.2d 1019 (1976).....	14
<i>R.M. Bacon, LLC v. Saint-Gobain Performance Plastics Corp.,</i> 959 F.3d 509 (2d Cir. 2020).....	14, 18
<i>Rudolph v. Hudson's Bay Co.,</i> No. 18-CV-8472 (PKC), 2019 WL 2023713 (S.D.N.Y. May 7, 2019).....	18
<i>Sacino v. Warwick Valley Cent. Sch. Dist.,</i> 138 A.D.3d 717, 29 N.Y.S.3d 57 (2016).....	13

<i>Sackin v. TransPerfect Glob., Inc.,</i> 278 F. Supp. 3d 739 (S.D.N.Y. 2017).....	18, 21
<i>Selby v. Principal Mut. Life Ins. Co.,</i> 197 F.R.D. 48 (S.D.N.Y. 2000)	23
<i>Shain v. Ellison,</i> 356 F.3d 211 (2d Cir. 2004).....	23
<i>Smahaj v. Retrieval-Masters Creditors Bureau, Inc.,</i> 69 Misc. 3d 597, 131 N.Y.S.3d 817 (2020).....	17
<i>Smith v. Pharos Sys. Int'l, Inc.,</i> No. 20-CV-1816-LJV, 2021 WL 4324415 (W.D.N.Y. Sept. 23, 2021).....	18, 19
<i>Sovereign Bank v. BJ's Wholesale Club, Inc.,</i> 533 F.3d 162 (3d Cir. 2008).....	18
<i>Spokeo, Inc. v. Robins,</i> 578 U.S. 330 (2016).....	5
<i>Thompson v. CRF-Cluster Model Program, LLC,</i> No. 19 CIV. 1360 (KPF), 2020 WL 4735300 (S.D.N.Y. Aug. 14, 2020)	23
<i>In re TJX Cos. Retail Sec. Breach Litig.,</i> 564 F.3d 489 (1st Cir. 2009).....	18
<i>TransUnion LLC v. Ramirez,</i> 141 S. Ct. 2190 (2021).....	6
<i>Wallace v. Health Quest Sys., Inc.,</i> No. 20 CV 545 (VB), 2021 WL 1109727 (S.D.N.Y. Mar. 23, 2021)	<i>passim</i>
<i>Whalen v. Michael Stores, Inc.,</i> 153 F. Supp. 3d 577 (E.D.N.Y. 2015)	6
<i>Whiteside v. Hover-Davis, Inc.,</i> 995 F.3d 315 (2d Cir. 2021).....	4
<i>Willingham v. Global Payments, Inc.,</i> No. 1:12-CV-01157, 2013 WL 440702 (N.D. Ga. Feb. 5, 2013)	9
<i>Worix v. MedAssets, Inc.,</i> 857 F. Supp. 2d 699 (N.D. Ill. 2012)	9
Statutes	
18 U.S.C.A. § 2722(b)	11

18 U.S.C. § 2702.....	9
18 U.S.C. § 2721.....	4, 7
18 U.S.C. §§ 2721-2725	10
18 U.S.C. § 2724(a)	1, 7
C.G.S.A. § 36a-701b(b)(1)(B)	24
Fed. R. Civ. P. 12(b)(1).....	2, 4
Fed. R. Civ. P. 12(b)(6).....	4
N.Y. Gen. Bus. Law § 899-aa, <i>et seq.</i>	17, 24
N.Y. Gen. Bus. Law § 349.....	2, 19, 20, 21

Defendant United Services Automobile Association (“USAA”) respectfully submits this Memorandum of Law in support of its Motion to Dismiss under Rules 12(b)(1) and 12(b)(6).

I. PRELIMINARY STATEMENT

The Court should dismiss Plaintiffs’ Complaint with prejudice because Plaintiffs fail to establish standing or state a claim for any substantive count or entitlement to any requested relief.

Article III Standing—Plaintiffs do not allege sufficient facts for an injury in fact based on the lack of sensitivity of the stolen driver’s licenses. A recent decision from the United States District Court for the Northern District of California dismissed a similar case for lack of standing where hackers also impersonated plaintiffs on an auto insurance quote website in order to steal plaintiffs’ driver’s license numbers, even when one of the plaintiffs alleged her stolen driver’s license was later used to apply for unemployment benefits in New York.

Drivers Privacy Protection Act (“DPPA”)—Plaintiffs cannot satisfy the DPPA’s knowledge requirement. Plaintiffs admit that their information was “stolen” by an unauthorized, cyber criminal from USAA in what they describe as a “Data Breach.” A fraudster impersonating Plaintiffs to steal Plaintiffs’ driver’s license numbers from USAA does not rise to the level of USAA “knowingly” disclosing such information under 18 U.S.C. § 2724(a).

Negligence—Plaintiffs fail to state a negligence claim because New York does not recognize claims for “negligent enablement of impostor fraud,” and USAA had no business relationship—or any relationship whatsoever with Plaintiffs—sufficient to impose a duty of care.

Negligence per se—Plaintiffs fail to state a negligence per se claim under New York law based on purported violations of Section 5 of the FTCA and New York’s Shield Act because neither statute authorizes private rights of action. Additionally, Plaintiffs’ negligence per se claim based on the federal DPPA fails with that claim.

Economic loss doctrine—Because Plaintiffs have not alleged physical injury or property damage, the economic loss doctrine bars all of Plaintiffs’ negligence-based claims.

GBL § 349—Plaintiffs fail to plead the requisite causation, as there are no allegations that Plaintiffs were specifically or generally aware of any of USAA’s information security statements, and the cause of any purported harm was the criminal and deceptive acts of a third party, not any supposed deception by USAA. Plaintiffs’ GBL § 349 claim also impermissibly rests on the alleged violations of other statutes that lack a private right of action.

Insufficient damages allegations—Plaintiffs do not allege any out-of-pocket expenses or monetary loss as a result of the incident and therefore fail to allege cognizable damages for their GBL § 349 and negligence-based claims.

Declaratory and Injunctive Relief—As an initial matter, such relief fails with Plaintiffs’ substantive claims. Even if any substantive claim were to survive, Plaintiffs impermissibly request relief relating to a past alleged injury, and any purported future injury is purely speculative. In any event, the declaratory relief would be improperly redundant and serve no useful purpose.

II. STATEMENT OF FACTUAL ALLEGATIONS

USAA provides, among other things, insurance services to members of the U.S. military and their families. Amended Consolidated Class Action Complaint (“ACAC”) ¶ 3. In that capacity USAA hosts a website where members can request an instant quote for auto insurance. *See* ACAC ¶ 38; Ex. A (Declaration of Jason M. Beach “Beach Decl.”) at Ex. 1 (template notification letter at 1).¹ Before seeking an instant auto insurance quote, the applicant must demonstrate USAA membership eligibility either by providing their membership credentials or

¹ In deciding USAA’s Rule 12 motions, the Court may consider documents that are “integral” and relied on in the complaint. *In re Merrill Lynch & Co.*, 273 F. Supp. 2d 351, 356 (S.D.N.Y. 2003) (Rule 12(b)(6)); *Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 145 (2d Cir. 2011) (Rule 12(b)(1)).

creating membership credentials. *See* ACAC ¶¶ 4, 35-36. To create membership credentials, an individual must provide significant information. *See* ACAC ¶ 9.

In early May 2021, the USAA instant automobile quote process was manipulated by cyber criminals, which the Complaint characterizes as a “Data Breach.” *E.g.*, ACAC ¶¶ 9, 11. Specifically, the cyber criminals used information about Plaintiffs to open unauthorized USAA memberships. *See* ACAC ¶ 9; Beach Decl. at Ex. 1 (template notification letter at 1). The criminals “likely obtained this personal information [of Plaintiffs] . . . elsewhere and used it to gain unauthorized access to [Plaintiffs’] driver’s license numbers” through the automated auto insurance quote process on USAA’s website. Beach Decl. at Ex. 1 (template notification letter at 1); *see* ACAC ¶ 43. Indeed, the information used to create the unauthorized USAA memberships must have been stolen elsewhere because Plaintiffs admit that they not only were “not previously USAA members” but also “had never provided USAA with any PII.” ACAC ¶ 9.

In other words, cyber criminals stole Plaintiffs’ personal information and then used it to impersonate Plaintiffs and create “fraudulent” USAA memberships in Plaintiffs’ names without their consent (ACAC ¶ 6). They then pivoted to the auto insurance quote feature where the criminals continued to impersonate Plaintiffs to steal their drivers’ license numbers from USAA (*id.* ¶ 9). As soon as USAA detected this unauthorized activity, it “blocked access to the driver’s license information” and notified Plaintiffs. Beach Decl. at Ex. 1 (template notification letter at 1). USAA also “notified law enforcement of the incident” and enhanced its security measures to help prevent this type of incident in the future. *Id.* Additionally, USAA offered Plaintiffs a complimentary two-year membership in Experian’s Identity Works program, which provides identity theft protection and resolution services. *Id.*

Plaintiffs Dolan and Mapes filed separate lawsuits which ultimately were consolidated in

this Court at the request of all parties. Plaintiffs filed a consolidated complaint, and now an amended complaint, alleging (1) violations of the federal Driver’s Privacy Protection Act (“DPPA”), 18 U.S.C. § 2721; (2) negligence; (3) negligence per se; (4) violations of GBL § 349, *et seq.*; and sought (5) declaratory and injunctive relief. Because the amended complaint includes the same dispositive legal deficiencies, USAA again moves to dismiss.

III. ARGUMENT

A. Standards of Review under Rules 12(b)(1) and 12(b)(6)

Rule 12(b)(1)—A court lacks subject-matter jurisdiction when a party lacks standing under Article III of the United States Constitution. *Wallace v. Health Quest Sys., Inc.*, No. 20 CV 545 (VB), 2021 WL 1109727, at *4 (S.D.N.Y. Mar. 23, 2021). A facial Rule 12(b)(1) challenge is based solely on the allegations of the complaint and “[t]he task of the district court is to determine whether the [complaint] alleges facts that affirmatively and plausibly suggest that the plaintiff has standing to sue.” *Id.* (quoting *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 56 (2d Cir. 2016)). The court must accept as true all material facts alleged in the complaint, but not argumentative inferences favorable to the party asserting jurisdiction. *Wallace*, 2021 WL 1109727, at *4.

Rule 12(b)(6)—A plaintiff’s complaint must “contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A plaintiff must “plead[] factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Whiteside v. Hover-Davis, Inc.*, 995 F.3d 315, 323–24 (2d Cir. 2021). In determining plausibility, a court considers “the full factual picture presented by the complaint, the particular cause of action and its elements, and the existence of alternative explanations so obvious that they render plaintiff’s inferences unreasonable.” *L-7 Designs, Inc. v. Old Navy, LLC*, 647 F.3d 419, 430 (2d Cir. 2011). A plaintiff’s barebones complaint and recitals of the elements

of causes of action “are not entitled to the assumption of truth and thus are not sufficient to withstand a motion to dismiss.” *Wallace*, 2021 WL 1109727, at *4.

B. Plaintiffs Lack Article III Standing

Plaintiffs’ fail to set forth an injury in fact, which is necessary to establish Article III standing. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992)). The sensitivity (or lack thereof) of data exposed alone can show lack of standing under the Second Circuit’s non-exhaustive, three-factor test to determine if a plaintiff has established an injury in fact from an unauthorized data disclosure. *Cooper v. Bonobos, Inc.*, No. 21-CV-854 (JMF), 2022 WL 170622, at *1 (S.D.N.Y. Jan. 19, 2022) (dismissing data exposure case on standing grounds and applying test set forth in *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 303 (2d Cir. 2021)).

Based on this data-sensitivity issue, a recent decision from the United States District Court for the Northern District of California dismissed a case for lack of standing based on a similar theft of drivers’ licenses from an auto insurance quote website. *Greenstein v. Noblr Reciprocal Exchange*, No. 21-cv-04537-JSW, 2022 WL 472183, at *1-2 (N.D. Cal. Feb. 15, 2022). Among other reasons, the court held that there was a lack of a concrete injury in fact because “driver’s license numbers do not provide hackers with a clear ability to commit fraud and are considered not as sensitive as social security numbers.” *Id.* at *4. Such information “is insufficient to open a new [financial] account in Plaintiffs’ names or to gain access to personal accounts likely to have more sensitive information.” *Id.* Indeed, just like here, one of the *Noblr* plaintiffs alleged that her “data was ‘fraudulently used to apply for unemployment benefits in New York.’” *Id.* at *5. This was not enough because the plaintiff “fail[ed] to demonstrate whether the [unemployment] application was successful or harmed her in any way.” *Id.* at *5, 8 (also stating that plaintiff “does

not allege she experienced any actual injury because of that application or any [un]employment benefits that may have been fraudulently obtained”).² Here, Plaintiff Dolan’s allegations suffer from the same deficiencies, and Plaintiff Mapes does not allege any harm from the alleged opening of an insurance policy in her name. *See* ACAC ¶ 67.³

As the *Noblr* court also held, allegations of time, effort, or money spent monitoring credit, *see* ACAC ¶ 113, likewise can be insufficient to establish standing. *See, e.g., Whalen v. Michael Stores, Inc.*, 153 F. Supp. 3d 577, 581 (E.D.N.Y. 2015) (granting motion to dismiss for lack of standing and explaining that “the Supreme Court has dismissed this type of argument, explaining that plaintiffs ‘cannot manufacture standing’ through credit monitoring”) (*quoting Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 416 (2013)). In both the *Cooper* and *Noblr* decisions, the courts also declined to find that plaintiffs’ expenditure of time and effort in monitoring credit reports established an injury in fact for purposes of a standing analysis. *Cooper*, 2022 WL 170622, at *5; *Noblr*, 2022 WL 472183, at *6.⁴

² USAA recognizes that other cases have found standing based on a disclosure that allegedly violated the DPPA. *E.g., Allen v. Verfore, Inc.*, No. 4:20-cv-04139, 2021 WL 3148870, at *1 (S.D. Tex. June 14, 2021). In addition to *Noblr*, at least one other federal court has questioned standing after *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210–13 (2021), of a proposed intervenor’s potentially insufficient harm allegations arising from the alleged disclosure of her personal information, noting that “her inclusion in the case might raise difficult issues related to the ‘concreteness’ of her injury and standing to sue.” *Hensley v. City of Charlotte*, No. 320CV00482KDBDSC, 2021 WL 4929491, at *4 (W.D.N.C. Oct. 21, 2021). Further, *Noblr* is factually indistinguishable from the instant case, at least from a standing analysis.

³ The allegations of traceability are also suspect. As explained above, Plaintiffs acknowledge that the criminals obtained significant amounts of their personal information from a source other than USAA. *E.g., ACAC ¶ 43.*

⁴ Should the Court disagree with the *Noblr* court and find that Plaintiffs Dolan and Mapes’ allegations are sufficient to demonstrate a concrete injury, this says nothing about whether any unnamed putative class members suffered such an injury. A class cannot include individuals who do not have Article III standing. *See TransUnion*, 141 S. Ct. at 2210–13 (holding that class members who did not suffer actual injury or sufficient risk of future harm do not have standing to sue).

C. USAA Did Not “Knowingly” Engage in Any DPPA Violative Conduct (Count III)

Plaintiffs allege that USAA violated the DPPA, 18 U.S.C. § 2721, *et seq.* The DPPA permits a civil action when the defendant: (1) “knowingly obtains, discloses[,] or uses personal information”; (2) “from a motor vehicle record”; and (3) “for a purpose not permitted under this chapter” 18 U.S.C. § 2724(a). *See also Luparello v. Inc. Vill. of Garden City*, 290 F. Supp. 2d 341, 344 (E.D.N.Y. 2003). The Complaint does not state a claim, as it fails to allege plausible facts that USAA’s conduct was done “knowingly.”

The DPPA requires that a defendant must “knowingly” engage in certain impermissible actions. 18 U.S.C. § 2724(a). Although there are many reported DPPA cases, very few address situations resulting from a criminal data breach. One such case, however, found that when a defendant is the victim of an information security incident in which a third-party criminal takes the protected information, such disclosure is not done “knowingly” by the victimized defendant. *Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654, 670–71 (E.D. Pa. 2015), *aff’d sub nom.*, 739 F. App’x 91 (3d Cir. 2018) (dismissing DPPA claim in data breach case, stating that “Defendants’ loss of Plaintiff’s [personal information due to criminal theft] did not constitute a ‘knowing disclosure’ . . . , which is a prerequisite to liability under the DPPA”).

Enslin was a putative class action arising from the criminal theft of fifty-five laptops allegedly containing the unencrypted, personal information of approximately 74,000 of the defendants’ then-current and former employees. *Id.* at 659. The information “included [the named] [p]laintiff’s Social Security number (‘SSN’), address, bank account information, credit card numbers, driver’s license information, and motor vehicle records.” *Id.* The plaintiff alleged that “various, unknown identity thieves were able to gain access” to his information from these laptops and then stole his identity. *Id.* Because the stolen information included his driver’s license information, the *Enslin* plaintiff also brought a DPPA claim. Similar to Plaintiffs here, the *Enslin*

plaintiff argued that the unauthorized taking of his personal driving information by criminals was a knowing DPPA disclosure to the criminals. The court rejected the argument.

[T]he Court is . . . unpersuaded by Plaintiff's argument that the theft of the [person's driving information ("PDI")] constituted a "knowing disclosure" by the . . . Defendants. . . . The theft of Plaintiff's PDI cannot be characterized as a "voluntary action" taken by the . . . Defendants to disclose that information. Under similar circumstances, the court in *Holmes v. Countrywide Fin. Corp.*, confronted with claims arising out of a loss of personal information after a data breach where "a ne'er-do-well independently stole [defendant's] customer information," held that under the Fair Credit Reporting Act, "no coherent understanding of the words 'furnished' or 'transmitted' " would give rise to liability under those circumstances. [No. 5:08-CV-00205-R,] 2012 WL 2873892, at *16 [(W.D. Ky. July 12, 2012)]. This Court considers the present situation to be analogous to *Holmes* and finds that "no coherent understanding" of the word "disclose" or "voluntary action" would include theft.

Enslin, 136 F. Supp. 3d at 671.⁵

In another data breach case, the United States District Court for the Southern District of Texas also granted a motion to dismiss for failure to state a claim under the DPPA. *See Allen*, 2021 WL 3144469, at *1 (adopting Magistrate Judge's report and recommendation); *Allen*, 2021 WL 3148870, at *1 (Magistrate Judge's report and recommendation). The *Allen* plaintiffs alleged a DPPA violation by Vertafore, a software company that provided support services for the insurance industry, after an unauthorized third party accessed data in Vertafore's possession. *See* 2021 WL 3148870, at *1. Finding that the complaint failed to allege the requisite knowledge under the DPPA, the *Allen* court explained:

The factual allegations also plainly state that anyone [who] may have obtained the data did so in an unauthorized manner, which undercuts the notion that Vertafore

⁵ Moreover, a number of federal courts have declined to impose DPPA liability even on individuals or entities who "indirectly facilitate[d] another's access of a motor vehicle record by maintaining an electronic database." *Doe v. Minn. Dep't of Pub. Safety Does (1-10)*, No. 17-4164(DSD/DTS), 2018 WL 1277005, at *3 (D. Minn. Mar. 12, 2018); *Nelson v. Jesson*, No. 13-340 (RHK/JJK), 2013 WL 5888235, at *3 (D. Minn. Nov. 1, 2013); *Kiminski v. Hunt*, Nos. 12-185, 13-208, 13-286, 13-358, 13-389, 2013 WL 6872425, at *9 (D. Minn. Sept. 20, 2013); *Enslin*, 136 F. Supp. 3d at 671–72; *Allen v. Vertfore, Inc.*, No. 4:20-cv-04139, 2021 WL 3144469, at *1 (S.D. Tex. July 23, 2021), *appeal docketed*, No. 21-20404, 2021 WL 314469 (5th Cir. Aug. 10, 2021).

knowingly disclosed the data to those unauthorized individuals

Id. at *4. In dismissing the claim, the court further stated that “[p]laintiffs’ allegation that Vertafore knowingly disclosed their personal information for an improper purpose is nothing more than a conclusory allegation or legal conclusion masquerading as a factual conclusion.” *Id.*

This “lack-of-knowledge” interpretation is further supported by other courts’ analyses of the knowledge requirements in analogous federal privacy statutes like the Stored Communications Act (“SCA”). *See* 18 U.S.C. § 2702, *et seq.* The SCA has an almost identical knowledge requirement (“knowingly divulged”), which is not met when the information is taken from the defendant by criminals, even if the defendant’s information security was allegedly insufficient. In *Worix v. MedAssets, Inc.*, 857 F. Supp. 2d 699, 703 (N.D. Ill. 2012), the court dismissed an SCA claim, as “the failure to take reasonable steps to safeguard data does not, without more, amount to divulging that data knowingly.” Similarly, in *Willingham v. Global Payments, Inc.*, No. 1:12-CV-01157, 2013 WL 440702, at *12 (N.D. Ga. Feb. 5, 2013), the court held that although the plaintiff alleged that the defendant “created or contributed to the breach of its data system,” such conduct did not constitute “knowingly divulg[ing]” information within the meaning of the SCA. The *Enslin* court made a similar finding that “privately holding PDI, even in an unsecured manner, does not constitute a ‘voluntary disclosure’ under the DPPA.” *Enslin*, 136 F. Supp. 3d at 671.⁶

Here, the allegations Plaintiffs make about the admittedly unauthorized and criminal theft of their information by cyber criminals show that USAA lacked—and could not as a matter of law

⁶ Plaintiffs seem to suggest that they satisfy the “knowingly” requirement because the criminals here committed their theft by fraudulently impersonating Plaintiffs rather than by hacking USAA’s systems. (ACAC ¶ 190.) The suggestion that some third-party criminal acts result in DPPA liability while other criminal acts do not has no support in the DPPA or the case law. Rather, this is part of Plaintiffs’ effort to turn the DPPA into a negligence statute, which it is not. *Kiminski*, 2013 WL 6872425, at *9 (comparing two statutes’ intent requirements to explain that the DPPA does not impose liability for mere negligence).

have had—the requisite knowledge under the DPPA. The Complaint asserts that cyber criminals first used Plaintiffs’ personal information to impersonate Plaintiffs and create “fraudulent” USAA memberships in Plaintiffs’ names without their consent (ACAC ¶¶ 6), and then pivoted to the auto insurance quote feature where the cyber criminals continued to impersonate Plaintiffs to steal their drivers’ license numbers from USAA (*id.* ¶ 9). *See also* ACAC ¶ 43, 48(c) (alleging scheme by which cybercriminals used “stolen information” from insurance companies). Indeed, the initial information that the cyber criminals used to create the unauthorized USAA memberships must have been stolen elsewhere because Plaintiffs admit that they not only were “not previously USAA members” but also they “had never provided USAA with any PII.” ACAC ¶ 9.

Significantly, other than conclusorily repeating the words of the DPPA, Plaintiffs never actually allege that USAA knowingly disclosed their drivers’ license information. Rather, Plaintiffs allege that USAA “knowingly and voluntarily configured and designed its insurance quote application portal on its website to disclose” this information. ACAC ¶ 185.⁷ In the context of the Complaint, it is clear that Plaintiffs are alleging that USAA was negligent because it allowed criminals to impersonate USAA members or potential members. But negligence, or even recklessness, is insufficient to impose liability under the DPPA.⁸ Consequently, allegations that USAA’s system was “designed” or “configured” (*e.g.*, ACAC ¶¶ 7, 12, 13, 19, 187, 189, 203) in

⁷ Plaintiffs also allege that the DPPA imposes “an obligation to use reasonable security measures.” ACAC ¶ 105. This allegation not only is an improper legal conclusion for evaluating a motion to dismiss, but also is wrong as a matter of law. Nothing in the entirety of the DPPA imposes an obligation to use information security measures. *See* 18 U.S.C. §§ 2721-2725.

⁸ DPPA’s knowledge “requirement is not compatible with a duty-of-reasonable-care/negligence standard.” *Loeffler v. City of Anoka*, No. 13-CV-2060 MJD/TNL, 2014 WL 4449674, at *6 (D. Minn. June 24, 2014), *report and recommendation adopted*, No. CIV. 13-2060 MJD/TNL, 2014 WL 4449692 (D. Minn. Sept. 9, 2014), *aff’d*, 893 F.3d 1082 (8th Cir. 2018); *Gulsvig v. Mille Lacs Cty.*, No. CIV. 13-1309 JRT/LIB, 2014 WL 1285785, at *6 (D. Minn. Mar. 31, 2014) (DPPA’s “*mens rea* requirement is ‘knowingly,’ not negligence); *Kiminski*, 2013 WL 6872425, at *9 (noting that DPPA does not impose liability for mere negligence).

a way to disclose information to cybercriminals does not constitute a “knowing” DPPA disclosure. *Allen*, 2021 WL 3148870, at *3 (rejecting that the requisite DPPA knowledge was established when “[i]n response to the commands of unauthorized individuals and consistent with the [way] they were programmed and configured by Vertafore, the unsecure servers disclosed Plaintiffs’ and Class members’ Driver’s License Information to the unauthorized individuals”)).

The argument that USAA “knowingly” disclosed Plaintiffs’ data is further undercut by another section of the DPPA, which addresses the very acts Plaintiffs allege here—obtaining personal information by fraud. But that section focuses on the conduct of the criminals, not the victims. 18 U.S.C.A. § 2722(b) (“It shall be unlawful for any person to make false representation to obtain any personal information from an individual’s motor vehicle record.”). It would be incongruous for Congress to (a) recognize that criminals will attempt to obtain personal information by fraud, (b) expressly make such conduct illegal, and (c) disclaim negligence as a basis for liability, yet make victims of the criminals’ actions liable for being victimized.

Under the facts as plead by the Plaintiffs, USAA did not violate the DPPA’s ban on knowing disclosure as a matter of law. The DPPA claim should be dismissed.

D. Plaintiffs Do Not State a Negligence Claim (Count I)

To plead a viable negligence claim under New York law, a plaintiff must plausibly allege that “(1) the defendant owed the plaintiff a cognizable duty of care; (2) the defendant breached that duty; and (3) the plaintiff suffered damage as a proximate result.” *Ferreira v. City of Binghamton*, 975 F.3d 255, 266 (2d Cir. 2020). Here, Plaintiffs fail to state negligence claims because New York law does not recognize claims for “negligent enablement of impostor fraud,” which is all Plaintiffs’ allegations amount to. Further, USAA has no duty of care to Plaintiffs, as Plaintiffs were not USAA members or customers and never entrusted any information to USAA.

1. New York does not recognize claims for “negligent enablement of impostor fraud”

Plaintiffs seek to impose a duty on USAA “under the common law” to exercise reasonable care in “obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.” ACAC ¶ 130. The Complaint makes clear that the entirety of Plaintiffs’ case stems from “[c]yber criminals [having] used Plaintiffs’ information [which was obtained elsewhere] to open fraudulent USAA membership accounts and request[ing] insurance quotes in Plaintiffs’ names” (*id.* ¶ 6) to steal Plaintiffs’ driver’s license numbers from USAA (*id.* ¶ 9). In other words, Plaintiffs’ negligence claim is that USAA negligently enabled the cyber criminals’ imposter fraud.

However, “New York does not recognize a cause of action for negligent enablement of impostor fraud.” *Polzer v. TRW, Inc.*, 256 A.D.2d 248, 248, 682 N.Y.S.2d 194, 195 (1998) (internal quotation marks omitted); *Bibicheff v. PayPal, Inc. (Bibicheff I)*, No. 217CV4679DRHAYS, 2020 WL 2113373, at *5 (E.D.N.Y. May 4, 2020) (citing *Polzer* and dismissing negligence claim brought under theory of negligent enablement of impostor fraud), *aff’d, Bibicheff v. PayPal, Inc. (Bibicheff II)*, 844 F. App’x 394, 396 (2d Cir. 2021) (summary order affirming lower court’s dismissal on this issue and citing *Polzer* with approval). In *Polzer*, for example, the Appellate Division affirmed the dismissal of a negligence claim against two credit card issuers for failing to detect that an imposter had fraudulently opened credit cards in the plaintiffs’ name. 256 A.D.2d at 238, 682 N.Y.S.2d at 195. *See also Bibicheff I*, 2020 WL 2113373, at *5 (citing to *Polzer* and dismissing a negligence claim against PayPal under a negligent enablement of impostor fraud theory); *Ladino v. Bank of Am.*, 52 A.D.3d 571, 574, 861 N.Y.S.2d 683, 687 (2008) (rejecting attempt to recover damages on the theory that defendant “negligently issued a loan to an imposter” because “New York does not recognize a cause of action for

‘negligent enablement of imposter fraud’’’).

2. USAA owes no duty of care to Plaintiffs with whom it has no relationship

A negligence claim must be “based on the breach of a legally cognizable duty of care.”

Abdulaziz v. McKinsey & Co., Inc., No. 21 CIV. 1219 (LGS), 2021 WL 4340405, at *4 (S.D.N.Y. Sept. 22, 2021) (citing *Sacino v. Warwick Valley Cent. Sch. Dist.*, 138 A.D.3d 717, 29 N.Y.S.3d 57, 60 (2016)). “Whether a defendant owed a duty of care to a plaintiff is a legal issue for the court.” *Abdulaziz*, 2021 WL 4340405, at *4. The Complaint implies that USAA’s purported duties arise from alleged foreseeable harm because, among other things,⁹ USAA “was on notice that a data breach was likely” from cyber security fraud alerts issued by the New York Department of Financial Services (NYDFS). ACAC ¶¶ 45-57.¹⁰ Plaintiffs also explicitly confirm that their theory is that “USAA had a common law duty to prevent *foreseeable* harm.” *Id.* ¶ 106 (emphasis added). But under New York law, “the court cannot recognize a duty based entirely on the foreseeability of the harm at issue.” *Abdulaziz*, 2021 WL 4340405, at *4 (quoting *In re N.Y. City*

⁹ The amended Complaint added allegations about publicly available Consent Orders from 2018 and 2020. *See generally* ACAC ¶¶ 58-63. The point of these additions is unclear. These consent orders were issued by a federal banking regulator and were entered into by USAA Federal Savings Bank, *not* by Defendant United Services Automobile Association. *Id.* (identifying language from the consent orders pertaining to “the Bank,” and not Defendant). Nor do Plaintiffs attempt to tie these irrelevant allegations to any aspect of their Complaint.

¹⁰ The NYDFS Cyber Fraud Alert gave recommendations that “NPI should not be displayed on public-facing websites” (*see, e.g.*, ACAC ¶ 50), but USAA’s online, instant insurance quote feature is not public facing. It can only be accessed by those who first have provided personal information to become members. *See* ACAC ¶¶ 4, 36 (alleging that before using their services, USAA requires users to become a USAA member and create an account). Indeed, to create membership credentials, an individual must provide significant information and answer qualifying questions about their military service. *See* ACAC ¶ 9 (“USAA provided Plaintiffs with a notice that . . . an unidentified third[]party illegally used some of Plaintiffs’ information, including their names and dates of birth, to obtain auto insurance quotes from [USAA’s] website.”); *id.* ¶ 37 (alleging that prospective members are asked qualifying membership questions). Plaintiffs’ contrary, hyperbolic, and conclusory allegations that USAA provided Plaintiffs’ PII “to anyone who requested an insurance quote” (*e.g.*, ACAC ¶ 185) does not even align with the specific allegations of their own Complaint.

Asbestos Litig., 27 N.Y.3d 765, 59 N.E.3d 458, 469 (2016)).¹¹

Plaintiffs' claim suffers for another reason. "Generally, there is no duty to control the conduct of third persons to prevent them from causing injury to others, . . . even where as a practical matter defendant can exercise such control." *Abdulaziz*, 2021 WL 4340405, at *4 (internal quotation marks omitted). However, "[a] duty may arise . . . where there is a relationship . . . between defendant and a third-person tortfeasor that encompasses defendant's actual control of the third person's actions." *Id.* (same). "Such relationships include master and servant, parent and child, and common carriers and their passengers." *Id.* (quoting *Oddo v. Queens Vill. Comm. for Mental Health for Jam. Cmtys. Adolescent Program, Inc.*, 28 N.Y.3d 731, 71 N.E.3d 946, 949 (2017)). In evaluating whether a duty exists, New York courts have "historically proceeded carefully and with reluctance to expand an existing duty of care." *Abdulaziz*, 2021 WL 4340405, at *4 (quoting *Davis v. S. Nassau Cmtys. Hosp.*, 26 N.Y.3d 563, 46 N.E.3d 614, 619 (2015) (collecting cases)). New York courts generally do not even impose a duty on businesses to protect their customers from the acts of third parties absent special circumstances. *Bibicheff II*, 844 F. App'x at 396. Here, Plaintiffs do not even allege they are USAA members or customers, ACAC ¶ 9, much less facts to support the type of special relationship contemplated under New York law to impose a duty here.

For example, *Bibicheff I* involved "allegedly fraudulent charges made with Plaintiff's credit cards through PayPal." 2020 WL 2113373, at *1. The "[p]laintiff held eighteen credit cards

¹¹ See also *Eiseman v. State*, 70 N.Y.2d, 175, 511 N.E.2d 1128, 1134 (1987) ("Foreseeability of injury does not determine the existence of duty."); *Pulka v. Edelman*, 40 N.Y.2d 781, 785, 358 N.E.2d 1019 (1976) ("Foreseeability should not be confused with duty.")). Consequently, "[a]bsent a duty running directly to the injured person there can be no liability in damages, however careless the conduct or foreseeable the harm." *R.M. Bacon, LLC v. Saint-Gobain Performance Plastics Corp.*, 959 F.3d 509, 516 (2d Cir. 2020) (internal quotation marks omitted and emphases in original).

... [that] were used for allegedly unauthorized transactions through twelve PayPal accounts "that the identity thief fraudulently created in [p]laintiff's name and/or business name and/or social security number, without her knowledge or approval." *Id.* The *Bibicheck I* court found that "PayPal had no special relationship with either Plaintiff or whoever stole her information to create the Fraudulent PayPal Accounts, and it therefore did not owe Plaintiff any duty." *Id.* Similarly, in the *Polzer* case, the court also noted that the plaintiffs failed to state a negligence claim because the defendants had no special relationship either with (a) the impostor who stole plaintiffs' credit information and fraudulently obtained credit cards, or (b) with plaintiffs, with whom Defendants stood simply in a creditor/debtor relationship. 682 N.Y.S.2d at 195.

Additionally, *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307 (S.D.N.Y. June 25, 2010), addressed a data exposure case in which unencrypted computer back-up tapes containing "names, addresses, Social Security numbers, bank account information, financial data, debit or credit card, checking account numbers and information and/or shareholder account information . . . w[ere] stolen, accessed and/or compromised by third parties while entrusted to Defendant." *Id.* at *2. In declining to impose a duty on the bank defendant, the *Hammond* court noted that "none of the named Plaintiffs had any direct dealings with Defendant." *Id.* at *11. Rather, the *Hammond* plaintiffs "had relationships (only) with institutional clients of Defendant, such as the Walt Disney Company, the Borough of Avalon, New Jersey, the American Water Company, and 'other establishments like the Vesper Club.' Plaintiffs gave their personal data over to those entities, which, in turn, forwarded the data to Defendant (which stored the data on the tapes that ultimately were lost or stolen)." *Id.* at *9.

Such "no-duty" results in these "no-relationship" cases apply with equal force here. USAA does not fall in the typical duty-to-control relationships such as master and servant, parent and

child, or common carrier and passenger. Plaintiffs here have no relationship whatsoever with USAA. Plaintiffs had not signed up to be USAA members, and they were not USAA customers. ACAC ¶ 9. In fact, Plaintiffs admit that they had never given any of their personal information to USAA. *Id.* Rather, cyber criminals who stole sensitive information from Plaintiffs elsewhere used that information to impersonate Plaintiffs and steal Plaintiffs' driver's license numbers through the automated auto insurance quote feature on a non-public portion of USAA's website. Similar to the results in the cases above, USAA does not owe any common-law duty of care to Plaintiffs here.

E. Plaintiffs Fail to State a Negligence Per Se Claim (Count II)

Plaintiffs allege negligence per se based on purported violations of the: (1) FTCA, (2) the DPPA, and (3) New York's Shield Act. ACAC ¶¶ 141-73. Each basis fails to state a claim.

First, “Section 5 [of the FTCA] does not provide a private right of action.” *In re GE/CBPS Data Breach Litig.*, No. 20 CIV. 2903 (KPF), 2021 WL 3406374, at *10 (S.D.N.Y. Aug. 4, 2021). “[I]nstead, the FTCA confers exclusive enforcement authority on the Federal Trade Commission,” so “Plaintiff’s negligence per se claim is not viable under New York law.” *Id.* (“join[ing] other courts in this District and State that have dismissed negligence per se claims predicated upon FTCA violations”). Courts in New York consistently dismiss negligence per se claims based on FTCA violations for this reason. *Cohen v. Ne. Radiology, P.C.*, No. 20 CV 1202 (VB), 2021 WL 293123, at *7 (S.D.N.Y. Jan. 28, 2021) (dismissing negligence per se claim and noting that “neither the parties nor the Court have identified a single case in this Circuit that has recognized that a private cause of action for negligence per se arises under New York law from violations of . . . the FTC Act. And several New York courts have concluded that . . . the FTC Act can[not] sustain a negligence per se claim.”).

Second, the specific section on which Plaintiffs rely in New York's Shield Act, § 899-bb, expressly states, “Nothing in this section shall create a private right of action.” New York courts

have consistently dismissed negligence per se claims based on the Shield Act's lack of a private right of action. *See Smahaj v. Retrieval-Masters Creditors Bureau, Inc.*, 69 Misc. 3d 597, 608, 131 N.Y.S.3d 817, 827 (2020) (dismissing negligence per se claim based on NY Shield Act §§ 899-aa, 899-bb); *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.*, 49 Misc. 3d 1027, 1037, 19 N.Y.S.3d 850, 858 (2015) (same under § 899-aa).

Third, for the same reasons that Plaintiffs' substantive DPPA claims fail, their derivative negligence per se claim based on the DPPA likewise fails. *See McFarlane v. Altice USA, Inc.*, 524 F. Supp. 3d 264, 282–83 (S.D.N.Y. 2021) (dismissing derivative negligence per se claim when substantive claim was dismissed).

F. The Economic Loss Doctrine Bars Plaintiffs' Negligence-Based Claims (Counts II and III)

Plaintiffs' negligence-based claims also are barred by the economic loss doctrine,¹² under which "a defendant is not liable in tort for purely economic loss unless the plaintiff demonstrates that the defendant owed a duty, which 'may arise from a special relationship[,] . . . to protect against the risk of harm to plaintiff.'" *Ambac Assurance Corp. v. U.S. Bank Nat'l Ass'n*, 328 F. Supp. 3d 141, 159 (S.D.N.Y. 2018) (quoting *532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc.*, 96 N.Y.2d 280, 292, 750 N.E.2d 1097, 1103 (2001)).¹³ Neither the Second Circuit nor the New York Court of Appeals has addressed whether the economic loss doctrine applies to data breach claims under New York law. In this vacuum, the doctrine's application in data

¹² Under New York law, the doctrine also applies to negligence per se claims. *E.g., Colangelo v. Champion Petfoods USA, Inc.*, No. 618CV1228LEKML, 2020 WL 777462, at *15 (N.D.N.Y. Feb. 18, 2020) (dismissing negligence and negligence per se claims under the economic loss doctrine).

¹³ There is "a sometimes inconsistent patchwork of state and federal decisions applying two related but distinct principles" under New York law regarding economic loss issues. *Ambac*, 328 F. Supp. 3d at 159. One principle is embodied in the "economic loss doctrine," which is addressed above. *Id.* (citing *532 Madison Ave. Gourmet Foods, Inc.*, 750 N.E.2d at 1101 n.1.) The other concerns "the economic loss rule," which is applied most often in the product liability context under New York law.

breach/exposure cases by federal courts in New York has been uneven. Certain cases in this district have refused to apply the economic loss doctrine because the defendant owed the plaintiffs a duty of care imposed by some other law, or categorically because the matter was not a product-liability case.¹⁴

The economic loss doctrine, however, has been applied to a variety of cases under New York law. *E.g., R.M. Bacon, LLC*, 959 F.3d at 516 (addressing environmental contamination) (citing *532 Madison Ave. Gourmet Foods, Inc.*, 96 N.Y.2d 280, 750 N.E.2d 1097 (applying doctrine to building construction collapse case)). Nor is there a persuasive basis to exclude data breach/exposure matters from an economic loss analysis as a bright-line rule.¹⁵ In a recent case involving a data exposure from the Western District of New York, the plaintiff claimed loss of business income due to an alleged software design that purportedly enabled third-party intrusion and invasion of privacy. *Smith v. Pharos Sys. Int'l, Inc.*, No. 20-CV-1816-LJV, 2021 WL 4324415, at *2 (W.D.N.Y. Sept. 23, 2021). The *Smith* court held that “[b]ecause [the Plaintiff]

¹⁴ *E.g., Wallace*, 2021 WL 1109727, at *9 (declining to apply economic loss rule in data breach case due to independent duty). However, several of these data breach cases appear to conflate the economic loss “rule” and economic loss “doctrine” to categorically exclude data breach cases from the economic loss doctrine’s reach. *E.g., Rudolph v. Hudson’s Bay Co.*, No. 18-CV-8472 (PKC), 2019 WL 2023713, at *9 (S.D.N.Y. May 7, 2019) (questioning the applicability of the economic loss doctrine outside the product-liability context); *Ambac Assurance Corp.*, 328 F. Supp. 3d at 159 (same); *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 749 (S.D.N.Y. 2017) (same).

¹⁵ That a case arises in the data breach/exposure context should not be a meaningful distinction in the application of the economic loss principles. They have been used in data breach/exposure cases around the country to bar negligence-based claims in the absence of physical injury or property loss. *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011) (dismissing negligence claims where plaintiffs allege merely economic losses); *see also Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 762 (C.D. Ill. 2020) (same); *Bellwether Cnty. Credit Union v. Chipotle Mexican Grill, Inc.*, 353 F. Supp. 3d 1070, 1085 (D. Colo. 2018) (same); *Cnty. Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 818 (7th Cir. 2018) (same); *Cumis Ins. Soc’y, Inc. v. BJ’s Wholesale Club, Inc.*, 455 Mass. 458, 918 N.E.2d 36, 46–47 (2009) (same); *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 498 (1st Cir. 2009), *as amended on reh’g in part* (May 5, 2009) (same); *Sovereign Bank v. BJ’s Wholesale Club, Inc.*, 533 F.3d 162, 175–77 (3d Cir. 2008) (same).

has not alleged that she suffered any personal injury or injury to her property, she has failed to state a viable [negligence] claim. . . .” *Id.*

Here, to the extent the Complaint can be construed to allege cognizable tort damages, they would be purely economic losses without any personal injury or property damage. *See, e.g.,* ACAC ¶¶ 138(a)-(i). Although the Complaint invokes several bases for purported independent duties owed to them by USAA, none states a claim. Nor do Plaintiffs allege any relationship with USAA, much less the type of special relationship required to skirt the economic loss doctrine. The economic loss doctrine therefore bars Plaintiffs’ negligence-based claims.¹⁶

G. Plaintiffs Fail to State a GBL § 349 Claim (Count IV)

“Section 349 of New York’s General Business Law prohibits deceptive acts or practices in the conduct of any business, trade, or commerce or in the furnishing of any service in New York.” *Bibicheff II*, 844 F. App’x at 396 (internal quotation marks omitted). “To maintain a cause of action under § 349, a plaintiff must show: (1) that the defendant’s conduct is ‘consumer oriented’; (2) that the defendant[] is engaged in a ‘deceptive act or practice’; and (3) that the plaintiff was injured by this practice.” *Id.* (same). Plaintiffs’ GBL § 349 claim fails for two reasons.

1. Plaintiffs fail to plead sufficient causation

Although private plaintiffs need not allege reliance for a GBL § 349 claim, they nevertheless must “show that the material deceptive act *caused* the injury.” *Doe v. Uber Techs., Inc.*, No. 20-CV-8446 (LJL), 2021 WL 3193166, at *19 (S.D.N.Y. July 28, 2021) (emphasis added). Failing to view a defendant’s allegedly deceptive representations until after the alleged

¹⁶ The allegations of the Complaint also suggest that the economic loss rule may apply, as Plaintiffs appear to assert a claim arising from negligent product design. Similar to the *Smith* case, which applied New York’s economic loss doctrine in a data exposure case that also involved negligent design, Plaintiffs here have alleged repeatedly that this incident was the result, of USAA’s flawed “online system configuration and design.” ACAC ¶ 13. *See also id.* ¶¶ 9, 38-40, 34, 65, 74, 75 (alleging defective design).

injury, for example, defeats any attempt to establish causation. *Bibicheff II*, 844 F. App’x at 396. *See also Gale v. Int’l Bus. Machines Corp.*, 9 A.D.3d 446, 447, 781 N.Y.S.2d 45, 47 (2004) (dismissing GBL § 349 claim due to insufficient causation when plaintiff did not see any of the allegedly deceptive statements before purchasing or acquiring product).

The *Bibicheff* plaintiff alleged “that PayPal, in derogation of its own policies and procedures with respect to suspicious and uncharacteristic account activity, failed to monitor and investigate twelve fake accounts created under Bibicheff’s name, business name, and/or social security number by her office manager, who defrauded her.” *Bibicheff II*, 844 F. App’x at 395. Affirming the trial court’s dismissal of the GBL § 349 claim, the Second Circuit held plaintiff’s “complaint fails to meet the [causation] prong of the GBL analysis, because it does not allege that she saw PayPal’s alleged misrepresentations until after the fraudulent activity and resulting harm had occurred.” *Id.* at 396. *See also Prignoli v. Bruczynski*, No. 20-CV-907 (MKB), 2021 WL 4443895, at *8 (E.D.N.Y. Sept. 28, 2021) (dismissing claim and finding that “[p]laintiff does not allege that Defendants made an affirmative representation to him that misled him, as he apparently had no contact with the Corporate Defendants and was not aware of their allegedly deceptive acts . . .”). Plaintiffs here also do not allege that they were specifically or generally aware of any of USAA’s information security statements, which warrants dismissal due to lack of causation.¹⁷

2. Other asserted statutory violations do not establish a GBL § 349 claim

Plaintiffs cannot base a GBL § 349 claim on purported violations of other statutes that do not provide a private right of action. *Conboy v. AT & T Corp.*, 241 F.3d 242, 258 (2d Cir. 2001)

¹⁷ Plaintiffs also allege that “Defendant states on its website that ‘[i]f you are a member and your Personal Information is ‘nonpublic personal information’ that we collect in connection with providing you a financial product or service, your Personal Information is . . . protected by our Privacy Promise.’” ACAC ¶ 79. Even if Plaintiffs had read USAA’s Privacy Promise, such statements only applied to USAA members. However, Plaintiffs admit they “did not sign up for USAA [membership] on their own.” *Id.*

(affirming dismissal of GBL § 349 claim based on violation of different state law statute that provided no private right of action); *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 777–78 (W.D.N.Y. 2017), *on reconsideration*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018), *order clarified*, 502 F. Supp. 3d 724 (W.D.N.Y. 2020) (dismissing “GBL § 349 claims, to the extent that they rest on . . . violations of statutes that do not authorize a private right of action”). Here, Plaintiffs base their GBL claims on alleged violations of Section 5 of the FTCA (*see* ACAC ¶ 198(e), (g), (i)) and the NY Shield Act (*see id.* ¶ 198(j)), neither of which provides a private cause of action. *See* Section III(D) above. Accordingly, neither statute can sustain a GBL § 349 claim.

H. Plaintiffs Fail to Allege Cognizable Damages (Counts II, III, and IV)

As explained above, Plaintiffs negligence and GBL claims require Plaintiffs to plead and prove actual injury. Plaintiffs have not sufficiently done so here.

Plaintiffs’ alleged injury is that they experienced identity theft after cyber criminals stole their driver’s license numbers. *E.g.*, ACAC ¶ 67 (alleging that an unauthorized insurance policy was taken out under Mapes name from a third-party provider and an unauthorized unemployment claim was made in Dolan’s name). But Plaintiffs do not allege these instances of alleged identity theft were more than attempted fraud. *See Wallace*, 2021 WL 1109727, at *7 (finding damages related to attempted fraud not cognizable). Nor do they allege that the attempted fraud caused them any specific, necessary, or reasonable out-of-pocket expenses or monetary loss. *See id.* (same and noting that no plaintiffs alleged “his or her bank account was drained”); *Sackin*, 278 F. Supp. 3d at 749 (finding that “reasonable mitigation steps” may establish a cognizable injury). For example, Plaintiff Dolan does not allege that the fraudulent unemployment application was successful or resulted in any financial or other injury to him. Nor does Plaintiff Mapes allege that the insurance policy fraudulently taken out under her name was successful or resulted in financial or other injury to her. The Complaint instead vaguely alleges that “Plaintiffs and [putative] Class

Members have had to spend, and will spend, and will continue to spend, significant time and money in the future to protect themselves” *Id.* ¶ 17.

To the extent such hazy allegations pertain to identity protection services, there are no allegations to support that such efforts were reasonable or necessary. Rather, the pleadings support that they are not because USAA already provided Plaintiffs with “a complimentary two-year membership” for identity protection services. *See* Beach Decl. at Ex. 1. To the extent Plaintiffs pin their injury to mitigation efforts to combat potential fraud in the future, Plaintiffs state that “many” putative class members “will incur out of pocket costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.” ACAC ¶ 113. But as this Court has recognized, costs to address speculative future injury do not rise to the level of cognizable damages. *Wallace*, 2021 WL 1109727 at *7 (similar allegations set forth non-cognizable damages where plaintiffs failed to “plausibly allege they are reasonably certain to incur *expenses* as a result of their greater exposure to fraud and identity theft”) (emphasis in original).

The additional allegations (*e.g.*, ACAC ¶¶ 23, 27) regarding purported “heightened risk for fraud and identity theft” that is “real and impending” are both speculative and conclusory. *See Wallace*, 2021 WL 1109727 at *8 (allegations merely suggest that plaintiffs may at some point incur fraud-related expenses). Nor is it reasonably certain that Plaintiffs would incur expenses for such protective measures because, again, USAA already offered complimentary identity theft protection services to Plaintiffs. Beach Decl. at Ex. 1 (template notification letter at 1). Moreover, merely spending time and energy monitoring for future instances of identity theft or mitigating the alleged fraud alone does not plead cognizable tort damages. *Wallace*, 2021 WL 1109727 at *7–8.

I. Plaintiffs Lack Sufficient Grounds for Declaratory or Injunctive Relief

The Court also should deny Plaintiffs' request for a declaratory judgment or an injunction for four reasons.

First, to the extent the Court finds that Plaintiffs do not state any substantive claim, derivative declaratory and injunctive relief must fail. *Norton v. Town of Islip*, 678 F. App'x 17, 22 (2d Cir. 2017) ("[T]he Declaratory Judgment Act is procedural only . . . and does not create an independent cause of action." (internal quotation marks omitted)); *Chiste v. Hotels.com L.P.*, 756 F. Supp. 2d 382, 406–07 (S.D.N.Y. 2010) (dismissing request for declaratory and injunctive relief and stating that "[d]eclaratory judgments and injunctions are remedies, not causes of action.").

Second, even if any substantive claim were to survive, Plaintiffs impermissibly request relief relating to, at most, a past alleged injury. A plaintiff seeking injunctive relief "must also prove that the identified injury in fact presents a 'real and immediate threat of future injury' often termed a 'likelihood of future harm.'" *Thompson v. CRF-Cluster Model Program, LLC*, No. 19 CIV. 1360 (KPF), 2020 WL 4735300, at *4 (S.D.N.Y. Aug. 14, 2020) (citing *Bernstein v. City of N. Y.*, 621 F. App'x 56, 57 (2d Cir. 2015) (summary order)); *Shain v. Ellison*, 356 F.3d 211, 215–16 (2d Cir. 2004). Where a complaint is "wholly devoid of any allegation that [the plaintiff] will likely be subject to future [harm] and thus immediately in danger of sustaining some direct injury," the claim for injunctive relief should be dismissed. *See Kanciper v. Lato*, No. 13CV00871ADSWDW, 2014 WL 12847274, at *2 (E.D.N.Y. Mar. 31, 2014) (internal quotations omitted).¹⁸ Past acts also do not create a "cloud of uncertainty affecting the Plaintiffs' rights that

¹⁸ Nor can Plaintiffs here attempt to bootstrap potential harm of any putative class member to satisfy their own standing for injunctive relief. *See Selby v. Principal Mut. Life Ins. Co.*, 197 F.R.D. 48, 64 (S.D.N.Y. 2000) (plaintiff who lacked standing for injunctive relief could not pursue such relief on behalf of a class).

can be lifted by a declaratory judgment.” *Chiste*, 756 F. Supp. 2d at 407 (“There is no basis for declaratory relief where only past acts are involved.”); *Nahabedian v. Intercloud Sys., Inc.*, No. 15-CV-00669(RA), 2016 WL 155084, at *6 (S.D.N.Y. Jan. 12, 2016) (dismissing declaratory judgment claim based on past acts).¹⁹ The alleged facts relate only to past acts.

Third, any alleged future injury is speculative. In an attempt to transmute past conduct into something more, Plaintiffs conclusorily allege that “the risk of another data breach is real, immediate, and substantial.” ACAC ¶ 210. But such allegations are no more than speculation and are insufficient. As the Fourth Circuit explained in the data breach context:

We acknowledge that the named plaintiffs have been victimized by “at least two admitted VA data breaches,” and that Ms. Watson’s information was compromised in both the 2013 laptop theft and the 2014 pathology reports theft. . . . But “[a]bsent a sufficient likelihood that [Plaintiffs] will again be wronged in a similar way,” . . . these past events, disconcerting as they may be, are not sufficient to confer standing to seek injunctive relief. . . . The most that can be reasonably inferred from the Plaintiffs’ allegations regarding the likelihood of another data breach at Dorn VAMC is that the Plaintiffs could be victimized by a future data breach. That alone is not enough.

Beck v. McDonald, 848 F.3d 262, 277–78 (4th Cir. 2017). *See also In re Brinker Data Incident Litig.*, No. 3:18-CV-686-J-32MCR, 2020 WL 4287270, at *3 (M.D. Fla. July 27, 2020) (rejecting declaratory relief claim when future hacking scenario “is possible, [but] too speculative to confer standing for declaratory and injunctive relief”); *Irwin v. Jimmy John’s Franchise, LLC*, 175 F. Supp. 3d 1064, 1074 (C.D. Ill. 2016) (dismissing declaratory relief when plaintiff “claims that she is at future risk of identity theft because other breaches may occur; however, that future risk is

¹⁹ Plaintiffs also request an order requiring USAA to provide identity theft protective services “for three (3) years.” ACAC ¶ 2. USAA is aware of no breach notification law in any U.S. State or territory—or any other law for that matter—that would impose such a requirement. Only a handful of state breach notification laws require credit monitoring at all, and New York is not one of them. *See generally* N.Y. Gen. Bus. Law § 899-aa, *et seq.* Of those limited jurisdictions, and only under specific circumstances, the longest time period imposed for credit monitoring is 24 months. *E.g.*, Conn. Gen. Stat. § 36a-701b(b)(1)(B). And even if this relief were cognizable, it can be provided through a damages remedy.

conjectural or hypothetical”). Here, Plaintiffs do not plausibly allege that use of their information specifically is subject to future misconduct by USAA, or that any such future harm (*see* ACAC ¶ 15) is more than mere speculation or conjecture. Moreover, Plaintiff Dolan’s prior Complaint conceded that USAA already has blocked access to the driver’s license information and is enhancing security measures to help prevent against fraudsters obtaining this information again (Dolan Compl. ¶ 13; *see also* Beach Decl. at Ex. 1 (template notification letter at 1), which makes any risk of future harm even more impermissibly speculative.

Fourth, USAA’s purported duties to Plaintiffs (*see* ACAC ¶ 208(a)-(b)) will be determined via Plaintiffs’ related substantive claims. The declaratory judgment request therefore is impermissibly duplicative and should be dismissed. *Id.* (dismissing duplicative declaratory judgment claim when it would serve no useful purpose); *Nahabedian*, 2016 WL 155084, at *5 (same); *McCulloch v. Town of Milan*, 559 F. App’x 96, 99 (2d Cir. 2014) (summary order affirming dismissal of redundant declaratory judgment request).

IV. CONCLUSION

For these reasons above, the Court should dismiss the Complaint.

Dated: February 18, 2022

Respectfully Submitted,

/s/ Armin Ghiam

Armin Ghiam
HUNTON ANDREWS KURTH LLP
200 Park Avenue
New York, NY 10166
Tel.: (212) 309-1000
Fax: (212) 309-1100
Email: aghiam@HuntonAK.com

Jason M. Beach
HUNTON ANDREWS KURTH LLP
Bank of America Plaza, Suite 4100
600 Peachtree Street, NE
Atlanta, Georgia 30308-2216
Tel.: (404) 888-4000
Email: jbeach@huntonAK.com

Neil K. Gilman
HUNTON ANDREWS KURTH LLP
2200 Pennsylvania Avenue, N.W.
Washington, DC 20037-1701
Tel.: (202) 955 15000
Email: ngilman@hunton.com

*Counsel for Defendant
USAA*

CERTIFICATE OF SERVICE

I hereby certify that, on February 18, 2022, I filed a true and correct copy of the foregoing document via the Court's electronic-filing system, which will send electronic notification of such filing to all counsel-of-record in this action.

/s/ Armin Ghiam

Armin Ghiam

HUNTON ANDREWS KURTH LLP